Facultad de Ingeniería y Ciencias Exactas

Seguridad e Integridad de la Información

Trabajo Práctico Grupal Obligatorio (TPO)

Primer Cuatrimestre 2025

Profesor: Carlos Mendoza

Fecha de Entrega: 16/06/2025

Integrantes: Martín Capece, Patricio Vecino, Sebastian Andres Deya, Santiago Tomas Loto y Felipe Vega Torre.

Índice

Alcance

Como grupo, determinamos una serie de objetivos para mantener un foco centralizado en lo que queríamos aprender. Seleccionamos esta temática por su creciente impacto en la economía digital y la seguridad informática actual. Hablando en términos generales, nuestro objetivo principal fue comprender el funcionamiento de la tecnología blockchain, ser capaces de identificar sus vulnerabilidades y analizar su impacto real en organizaciones y usuarios. A partir de esto, desglosamos los siguientes objetivos específicos a detallar:

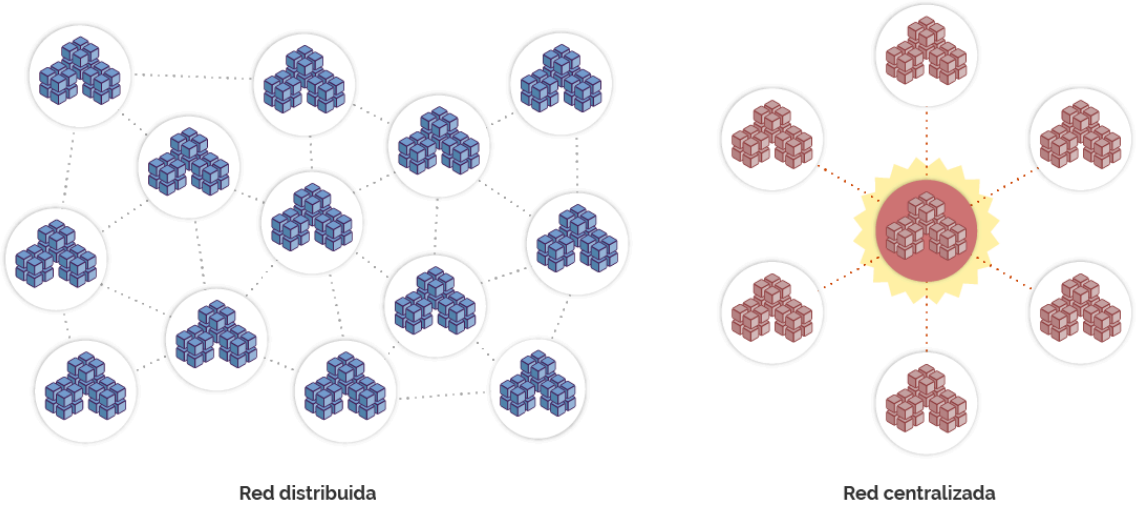
- Realizar una introducción al mundo de blockchain y Web3.
- Reconocer las principales vulnerabilidades presentes en este entorno.
- Analizar situaciones reales en las que dichas vulnerabilidades fueron explotadas, detallando los mecanismos de ataque y su impacto.
- Distinguir los distintos tipos de costos que pueden generarse en una empresa a raíz de estas amenazas, ya sean económicos, reputacionales, legales, entre otros.
- Explorar posibles soluciones, buenas prácticas y estrategias de mitigación que permitan reducir los riesgos identificados.

Ataques a Blockchain

Introducción sobre Blockchain y Web3

Blockchain

Blockchain es una tecnología de registro distribuido (DLT, por sus siglas en inglés) que permite almacenar información de manera segura, transparente e inmutable. En lugar de estar almacenados en un único servidor centralizado, los datos se distribuyen a través de una red de nodos que validan y registran transacciones en bloques. Cada bloque está enlazado criptográficamente al anterior, formando una "cadena" que es extremadamente difícil de alterar sin el consenso de la mayoría de los nodos.



Red distribuida

Red centralizada

Características principales:

- Descentralización: No existe un control único sobre la red.
- Inmutabilidad: Una vez que un bloque es agregado, no puede ser modificado sin alterar toda la cadena.
- Transparencia: Las transacciones son visibles para todos los participantes.
- Seguridad: Uso intensivo de criptografía para garantizar la integridad de la información.

La blockchain no solo soporta criptomonedas como Bitcoin o Ethereum, sino también contratos inteligentes (smart contracts), sistemas de votación, cadenas de suministro y mucho más.

Gran parte de la seguridad de la información en Blockchain se debe al uso de métodos criptográficos para encriptarla, y una de las principales herramientas para hacerlo son los llamados Hash, o digestos criptográficos. Un hash es un código que se obtiene al procesar información a través de una función. Si modificamos aunque sea algo muy pequeño de esa información, como el color de una foto, o simplemente agregar un acento en un documento de texto, el hash va a cambiar completamente. Los hash suelen llamarse digestos o resúmenes, porque normalmente tienen un tamaño fijo y de pocos dígitos, por ejemplo 64 caracteres en SHA-256

Los hash criptográficos que mencionamos anteriormente no solo sirven para garantizar la integridad de la información, sino que también juegan un papel fundamental en el proceso de sellado de bloques, que es como las transacciones se confirman y añaden permanentemente a la blockchain.

El sellado de bloques es el mecanismo mediante el cual los participantes de la red (mineros o validadores) toman un conjunto de transacciones pendientes, las organizan en un bloque, y lo añaden a la cadena. Para que este proceso sea seguro y confiable, la red debe ponerse de acuerdo sobre qué bloques son válidos. Esto se logra a través de mecanismos de consenso.

Proof of Work (PoW)

En el sistema Proof of Work, los mineros compiten para resolver un problema matemático que involucra encontrar un hash específico. Deben encontrar un número (llamado nonce) que, al combinarse con los datos del bloque y procesarse con SHA-256, produzca un hash que comience con una cantidad determinada de ceros. Este proceso requiere mucha potencia computacional, y el primer minero en encontrar la solución obtiene el derecho de añadir el bloque a la cadena y recibe una recompensa. Bitcoin utiliza este mecanismo.

Proof of Authority (PoA)

En contraste, el Proof of Authority funciona con un conjunto preaprobado de validadores conocidos que se turnan para crear bloques. No hay competencia computacional, sino que la validez se basa en la reputación e identidad de estos validadores. Este sistema es más eficiente energéticamente y se usa principalmente en redes privadas o de consorcio.

Las Criptomonedas son justamente monedas virtuales que se basan en cadenas de bloques para controlar la creación de unidades y verificar la transferencia de activos

entre los usuarios. Como todas las divisas, su valor en gran parte está basado en la confianza que los usuarios ponen en ella. Pero al tener la particularidad de depender de Blockchain, esa confianza se apoya en las garantías que da la tecnología, en la criptografía, no en entidades centralizadoras, como un Banco Central.

La utilidad principal de las criptomonedas es el envío de valor mediante un sistema completamente seguro y digital. Cada cripto tiene una cotización propia que se basa en su oferta y demanda. Todas ellas puedan ser enviadas entre usuarios sin problemas e intercambiar valor en forma digital.

Por otro lado, los Smart Contracts son más bien flujos de tareas programables dentro de Blockchain, que abren la posibilidad de desarrollar aplicaciones.

A diferencia de una App tradicional, donde tenemos que confiar en las garantías que nos da su desarrollador, en un smart contract es posible programar un flujo de tareas pre establecido entre partes interesadas, apoyado en todas las garantías de confianza y transparencia que nos da una red de cadena de bloques.

Gracias a los smart contracts se pueden realizar tareas cada vez más complejas. Así, podemos dejar de pensar en Blockchain como un mero registro y comenzar a pensar procesos como seguimiento de licitaciones, sistemas de trazabilidad de productos, plataformas de documentos “vivos”, y mucho más.

En otras palabras, un “contrato inteligente” es un programa que se ejecuta automáticamente cuando se cumplen ciertas condiciones, y que está almacenado en una blockchain. La diferencia clave con un contrato tradicional es que no necesita intermediarios: el código hace cumplir las reglas sin que nadie tenga que intervenir ni pueda manipularlo.

Un claro ejemplo de este último es el de un “Intercambio seguro de activos digitales entre dos personas”. En donde dos personas, que no se conocen ni confían entre sí, quieren intercambiar activos digitales (como E-books, Códigos de Acceso a Plataformas, Licencias de Software, etc). Si la persona “A” envía su parte primero, corre el riesgo de que la persona “B” no cumpla. Y viceversa. Así entonces, se crea un contrato inteligente en la blockchain con las siguientes reglas:

- “Cuando “A” envíe su activo digital al contrato, y “B” envíe el suyo, el contrato hará el intercambio automáticamente.”
- “Si una de las partes no envía su parte en 24 horas, se devuelve lo que fue enviado.”

De esta manera, no hay intermediarios, así disminuye las posibilidades de estafa si el contrato está correctamente programado y auditado, todo se hace en segundos, sin que nadie lo pueda alterar.

Web3

Web3 refiere a la evolución de Internet que incorpora blockchain para lograr un ecosistema más descentralizado y transparente.
A diferencia de Web1 (estática, lectura) y Web2 (dinámica, interacción controlada por grandes plataformas como Google o Facebook), Web3 busca empoderar a los usuarios, dándoles control sobre su identidad, sus datos y sus activos digitales.

Características principales:

- Criptomonedas y Tokens: Representan valor o derechos en un ecosistema descentralizado.

- Smart Contracts: Programas que se ejecutan automáticamente cuando se cumplen ciertas condiciones.

- DAOs (Organizaciones Autónomas Descentralizadas): Organizaciones gobernadas por reglas codificadas en contratos inteligentes, sin una autoridad central.

- NFTs (Tokens No Fungibles): Representaciones digitales únicas de activos.

Web3 está profundamente interconectada con blockchain, ya que utiliza esta tecnología como base para todas sus aplicaciones.

Relación entre estos conceptos con ataques cibernéticos

Aunque blockchain y Web3 introducen mejoras enormes en términos de seguridad y transparencia, no están exentos de riesgos.
Debido a su valor financiero (criptomonedas, tokens), su naturaleza descentralizada y la complejidad técnica de sus aplicaciones (smart contracts, DAOs), se han convertido en objetivos atractivos para ciberdelincuentes.

Principales tipos de ataques en el ecosistema Blockchain/Web3:

- Exploits de Smart Contracts: Errores de código en contratos inteligentes que pueden ser explotados para robar fondos.

- Ataques del 51%: Cuando un grupo controla más del 50% del poder de cómputo de la red y puede manipular transacciones.

- Phishing y Suplantación de Identidad: Robos de claves privadas a usuarios desprevenidos.

- Ataques de Puentes (Bridges): Vulnerabilidades en los sistemas que conectan distintas blockchains.

- Reentrancy Attacks: Ataques donde un contrato inteligente es llamado repetidamente antes de que finalice la primera ejecución, permitiendo el drenaje de fondos (famoso caso de *The DAO*).

- Rug Pulls: Estafas donde desarrolladores abandonan un proyecto Web3 llevándose todos los fondos de los inversores.

En resumen, mientras blockchain y Web3 abren el camino hacia un internet más justo y descentralizado, también traen nuevos desafíos de seguridad que requieren atención crítica. Esto nos permitirá introducirnos a diferentes ejemplos, que demuestran la premisa anterior:

Hackeo al puente Ronin de Axie Infinity (2022)

Descripción del ataque:
Axie Infinity, un videojuego basado en la tecnología blockchain que tuvo un gran auge entre finales de 2021 y principios de 2022, utilizaba un puente llamado Ronin Bridge para facilitar las transferencias de criptomonedas entre diversas blockchains, especialmente Ethereum. Este puente era esencial para que los jugadores pudieran mover activos digitales como AXS (Axie Infinity Shards) y SLP (Smooth Love Potion) dentro y fuera del ecosistema del juego.

En marzo de 2022, el grupo de hackers Lazarus, que se cree que está vinculado al gobierno de Corea del Norte, logró comprometer 5 de las 9 claves privadas necesarias para validar las transacciones en el puente Ronin. Con este acceso mayoritario (Ataque del 51%), pudieron autorizar transacciones fraudulentas y robar aproximadamente 620 millones de dólares en criptomonedas (principalmente ETH y USDC).

Causas del ataque en blockchain:
Lo que falló en este caso fue la gestión y protección de las claves privadas utilizadas en el puente Ronin.

- El sistema de validación de transacciones del puente Ronin dependía de la autorización de claves privadas, y un control mayoritario de estas claves por parte de los atacantes les permitió autorizar transacciones fraudulentas sin ser detectados.

- La falta de una infraestructura más segura para la gestión de claves privadas y la auditoría de seguridad en el diseño del puente permitió que el ataque fuera exitoso.

Costos identificados:

- Caída en la confianza: La comunidad de Axie Infinity sufrió una pérdida de confianza masiva, ya que el juego dependía de la estabilidad económica y la integridad del puente para que los jugadores pudieran mover sus activos.

- Caída en el precio de las monedas: El precio de AXS cayó de más de 160 USD en noviembre de 2021 a menos de 20 USD tras el hackeo. El token SLP también perdió su valor debido a una sobreproducción y a la percepción de vulnerabilidad en el modelo económico del juego.

- Congelamiento del puente Ronin: El puente Ronin se cerró temporalmente para reforzar su seguridad, lo que causó inconvenientes a los jugadores e inversores que no podían mover sus fondos.

The DAO Hack (2016)

Descripción del ataque:
The DAO fue un fondo de inversión descentralizado basado en Ethereum que permitió a los usuarios votar sobre qué proyectos financiar a cambio de tokens. Los usuarios podían invertir en The DAO y recibir ganancias de los proyectos seleccionados. The DAO recaudó más de 150 millones de dólares en Ether, convirtiéndose en una de las mayores ofertas de financiación colectiva en la historia de las criptomonedas hasta ese momento.

En junio de 2016, un atacante explotó una vulnerabilidad en el código del contrato inteligente de The DAO mediante un ataque de reentrancia, una técnica en la que el atacante envía una llamada recursiva a un contrato antes de que el primer estado de la transacción sea registrado. Esto le permitió retirar fondos repetidamente del contrato inteligente de The DAO sin que el contrato pudiera detectar la cantidad extraída. El atacante logró robar 50 millones de dólares en Ether, lo que representaba aproximadamente el 30% del fondo total de The DAO.

Básicamente, el ataque fue posible debido a un error en el código del contrato inteligente que no validaba correctamente las transacciones. La vulnerabilidad permitía a los atacantes realizar una llamada recursiva al contrato, lo que les permitió extraer más Ether del que realmente les correspondía.

Consecuencias y costos generados por el ataque:

- Bifurcación de Ethereum (Hard Fork): En respuesta al ataque, la comunidad de Ethereum decidió realizar una bifurcación para revertir las transacciones fraudulentas y devolver los fondos a los inversores originales de The DAO. Esto resultó en la creación de dos versiones de Ethereum: Ethereum (ETH) y Ethereum Classic (ETC). La bifurcación dividió a la comunidad de Ethereum y generó controversia sobre si las blockchains deben o no ser alteradas para resolver problemas como este.
- Pérdida de confianza: El ataque y la posterior bifurcación generaron desconfianza entre muchos usuarios, que cuestionaron la inmutabilidad de las blockchains, uno de los principios fundamentales de las criptomonedas.

- División de la comunidad: La bifurcación creó dos cadenas separadas, lo que causó una disputa filosófica sobre el papel de la descentralización y la interferencia de los desarrolladores en una blockchain.
- Impacto en la adopción de smart contracts: La confianza en los contratos inteligentes se vio afectada, y las plataformas basadas en smart contracts tuvieron que trabajar más para demostrar que sus contratos eran seguros y audibles.

Ataque a Poly Network (2021)

Descripción del ataque:

Poly Network es un protocolo de interoperabilidad que permite la transferencia de activos entre diferentes blockchains como Ethereum, Binance Smart Chain y Polygon. El 10 de agosto de 2021, un hacker logró explotar una vulnerabilidad crítica en los contratos inteligentes de Poly Network, lo que le permitió redirigir fondos a direcciones bajo su control.

El atacante logró manipular los contratos del protocolo para modificar los "guardianes" (keepers) que verifican y autorizan las transacciones entre cadenas. Al alterar estos guardianes, el hacker pudo falsificar mensajes entre blockchains y autorizar transferencias fraudulentas, robando aproximadamente $611 millones en distintas criptomonedas (ETH, BNB, USDC, entre otras).

Costos identificados:

Impacto financiero directo:

- Pérdida temporal de $611 millones en activos digitales.
- Costos operativos y técnicos para la recuperación y reparación del protocolo.
- Gastos en auditorías forenses y de seguridad posteriores.

Impacto reputacional:

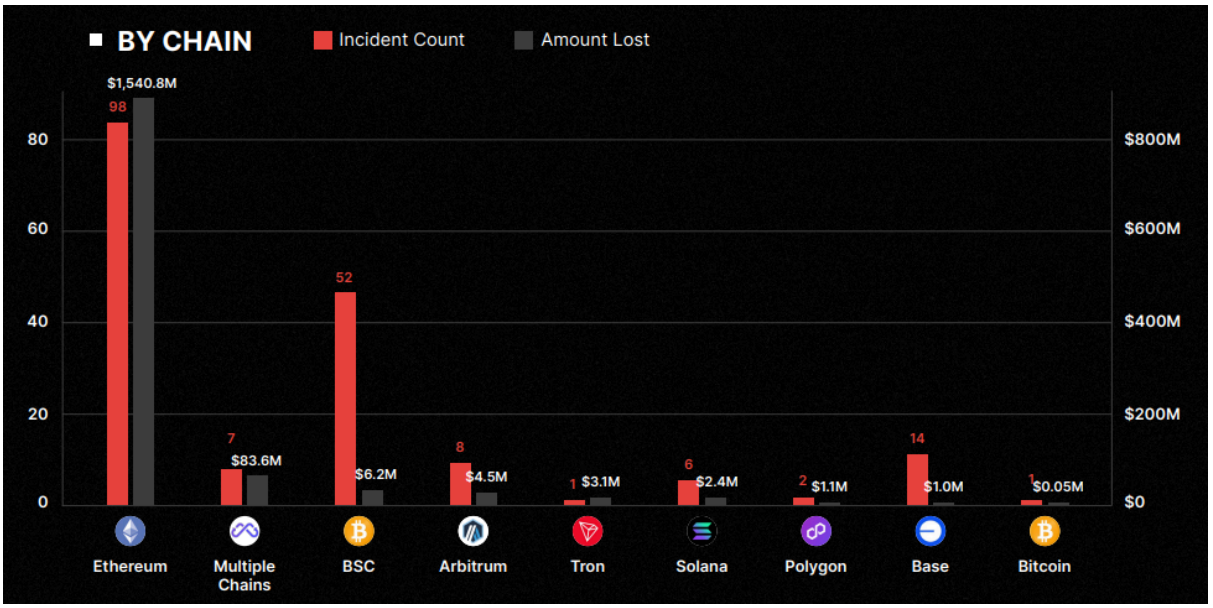
- Severo daño a la confianza en Poly Network como protocolo de interoperabilidad seguro.
- Cuestionamiento sobre la madurez y seguridad del ecosistema DeFi en general.
- Escepticismo sobre la seguridad de los puentes cross-chain.

Una particularidad de este caso es que el atacante, autodenominado "Mr. White Hat", comenzó a devolver los fondos el día siguiente al ataque, alegando que había realizado el hackeo con fines educativos para exponer la vulnerabilidad. Dentro de las dos semanas siguientes, el 100% de los fondos fueron devueltos a Poly Network. La empresa llegó a ofrecer al hacker un puesto como "Asesor de Seguridad" y dinero para no revelar la vulnerabilidad, el cual fue entregado a proyectos técnicos.

Graficos y Estadisticas (2025 Q1)

Para complementar el análisis teórico de las vulnerabilidades en blockchain, incorporamos una sección basada en datos estadísticos recientes que reflejan el impacto real de los ataques. Esta información nos permite dimensionar la magnitud de los riesgos.

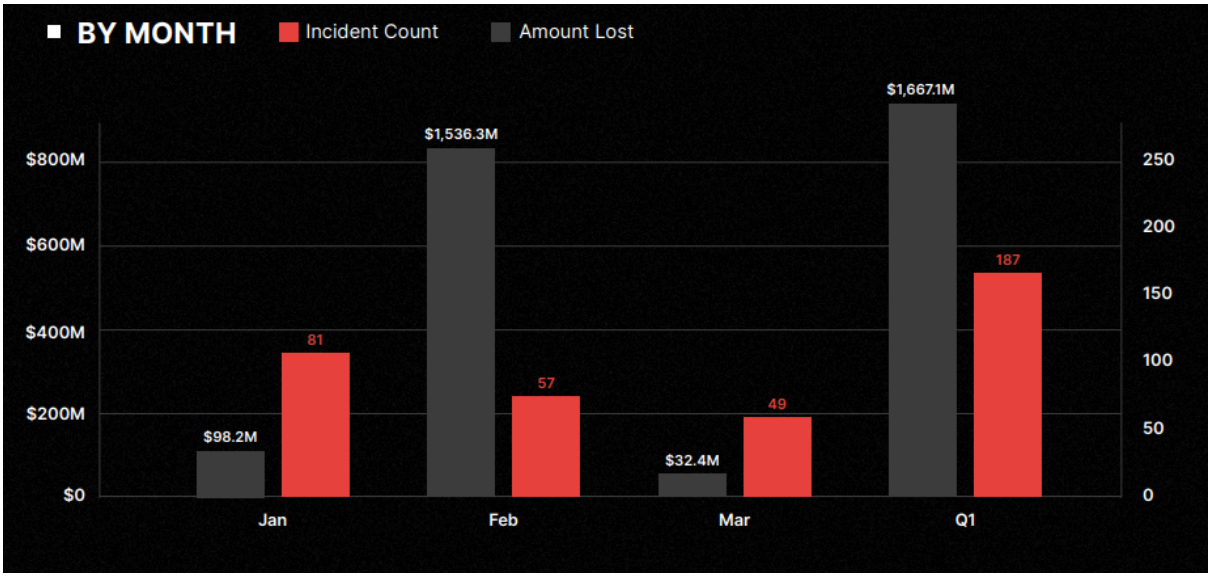
El objetivo de esta sección es brindar un panorama visual, junto con un análisis para poder comprender lo que estamos viendo, a través de gráficos de cifras analizadas que corresponden al primer trimestre del año 2025.



Se ve claro que Ethereum fue la red más atacada, tanto en cantidad de incidentes como en dinero robado. No es casualidad: es la blockchain más usada para contratos inteligentes y DeFi, así que también es la que más atrae a los atacantes.

Otras redes como Binance Smart Chain, Polygon o Solana también aparecen en el gráfico, pero con mucho menos impacto. Esto muestra que los hackers apuntan donde hay más movimiento y más valor.

Entonces podemos decir que las redes más grandes y populares también son las más vulnerables, si no se toman medidas de seguridad adecuadas.



Lo que más llama la atención en este gráfico es cómo febrero concentra casi todo el dinero robado en el trimestre. Aunque hubo más de 180 incidentes en total, el mayor impacto económico se dio en ese mes puntual, donde ocurrió uno de los hackeos más grandes registrados. (Bybit)

Enero y febrero también tuvieron ataques, pero el monto que se perdió fue mucho menor. Esto nos muestra que no siempre importa cuántos ataques hay, sino qué tan graves son. A veces, un solo caso puede generar un daño enorme.

Conclusión

Al terminar este trabajo práctico, como grupo sentimos que nuestra forma de ver el mundo de blockchain y Web3 cambió bastante. Al principio, muchos de nosotros sólo conocíamos lo básico y pensábamos que estas tecnologías estaban más relacionadas con la especulación o eran solo una moda pasajera. Pero al investigar más a fondo, nos dimos cuenta de que detrás hay mucha tecnología compleja y un gran potencial real.

Durante el desarrollo del TPO, uno de los desafíos fue entender bien cómo funciona todo a nivel técnico y, al mismo tiempo, poder explicarlo de forma clara y sencilla. Esto nos llevó a investigar no sólo qué eran las vulnerabilidades, sino también cómo ocurren y por qué son un problema.

Una de las cosas que más nos sorprendió fue darnos cuenta de una especie de contradicción en el mundo blockchain: aunque la tecnología en sí es muy segura, las aplicaciones que se crean sobre ella pueden tener muchas fallas. Casos como los de The DAO, Ronin Bridge y Poly Network muestran cómo errores en la programación pueden poner en riesgo millones de dólares.

Analizando estos ataques, entendimos que la mayoría de las fallas no están en la criptografía o en la base del sistema, sino en errores humanos al diseñar o programar contratos inteligentes. Esto demuestra lo importante que son las auditorías, las pruebas y también la educación de quienes usan o desarrollan estas herramientas.

Antes del TPO veíamos blockchain como algo con mucho "hype", pero poca utilidad real y lleno de riesgos. Ahora entendemos que es una tecnología con mucho futuro, que puede ser tan crítica como el sistema bancario, y que necesita una seguridad muy bien pensada, sobre todo porque todo queda grabado y no se puede cambiar.

Bibliografía

Hack3d Report. (2025). Recuperado de https://www.certik.com/resources/blog/hack3d-the-web3-security-quarterly-report-q1-2025

Ataques a blockchain. Recuperado de https://wesecureapp.com/blog/attacks-on-blockchain/

Chainalysis. El hackeo del puente Ronin de Axie Infinity: cómo el Grupo Lazarus de Corea del Norte robó 600 millones de dólares y cómo Chainalysis ayudó a recuperar 30 millones. Recuperado de https://www.chainalysis.com/blog/axie-infinity-ronin-bridge-dprk-hack-seizure/

Lyngaas, S. (2022, 14 de abril). EE. UU. vincula a Corea del Norte con el robo de 600 millones de dólares en Axie Infinity. The Washington Post. Recuperado de https://www.washingtonpost.com/technology/2022/04/14/us-links-axie-crypto-heist-north-korea/

Nelson, D. (2022, 24 de junio). El desarrollador de Axie Infinity, Sky Mavis, reembolsará a las víctimas del hackeo de Ronin Bridge. CoinDesk. Recuperado de https://www.coindesk.com/business/2022/06/24/axie-infinity-developer-sky-mavis-to-reimburse-victims-of-ronin-bridge-hack

Chainlink. Ataques de reentrada y el hackeo de The DAO. Recuperado de https://blog.chain.link/reentrancy-attacks-and-the-dao-hack/

Wikipedia. The DAO. Recuperado de https://es.wikipedia.org/wiki/The_DAO

BeInCrypto. El hackeo de The DAO explicado. Recuperado de https://beincrypto.com/learn/dao-hack-explained/

Reuters. (2021, 12 de agosto). Cómo los hackers robaron 613 millones en tokens de criptomonedas de Poly Network. Recuperado de https://www.reuters.com/technology/how-hackers-stole-613-million-crypto-tokens-poly-network-2021-08-12/

CoinDesk. (2021, 10 de agosto). Plataforma DeFi entre cadenas Poly Network hackeada. Recuperado de https://www.coindesk.com/markets/2021/08/10/cross-chain-defi-site-poly-network-hacked-hundreds-of-millions-potentially-lost/

IBM. Qué es la tecnología blockchain. Recuperado de https://www.ibm.com/think/topics/blockchain

Investopedia. (s. f.). Contratos inteligentes. Recuperado de https://www.investopedia.com/terms/s/smart-contracts.asp